THE UNIVERSITY OF NORTH CAROLINA SYSTEM

UNC System-Wide **Standard on Information Technology**

User Identity and Access Control **Version Effective Date:07-15-2020**

CONTENTS

1. INTRODUCTION

1.1 Background and Purpose

The University of North Carolina Board of Governors (BoG) mandated this Standard via their policy 1400.3. The purpose of this document is to present a Standard that all University of North Carolina System (UNC System) constituent institutions must follow as set forth in this document for risk-based implementation of user identity confirmation and access control to University information.

1.2 Coverage and Scope

This University of North Carolina System (UNC System) Standard is issued pursuant to Board of Governors (BoG) policy 1400.3. It applies to all constituent institutions of the UNC System and all constituents of those institutions.

2. STANDARD

2.1 User Identification and Authentication

Each institution shall implement multi-factor authentication (MFA) and other measures (including policies, standards or procedures) that meet or exceed BoG 1400.3 and this Standard to protect sensitive information (SI) as defined below. If an institution is unable to implement MFA to protect SI, the Senior Officer with Information Security Responsibility (Senior Officer), as described in BoG policy 1400.2 or other party designated in written form (electronic acceptable), must identify, implement and document alternative techniques and/or measures to protect sensitive information (SI) or document to the UNC System CIO additional resources needed as described below. Within 6 months of the effective date of this UNC System Standard (i.e., due 1/15/21) and every 3 years thereafter, Senior Officers must send to the CIO of the UNC System (see 7.1-primary contact) a document that provides detail regarding the respective institution's user identity and access control program including techniques and/or measures implemented to protect SI, as defined in the constituent institution's Information Classification policy (or similar) or establish documentation of relevant risk assessment and acceptance by a governance group that meets the requirements of BoG 1400.1. The document must include any alternatives to MFA as well as residual risk retained due to lack of resources. The above documents will support the CIO's evaluation of program adequacy such that the CIO may identify institutions requiring additional resources to meet the requirements of 1400.3.

2.2 Access Controls

Access controls must be appropriate to the sensitivity of the information to be protected, in keeping with Information classification documentation relevant to each institution and must include consideration of the principle of least privilege.

Mechanisms to control access to SI must include at a minimum the following methods:

2.2.1 Authorization

All initial issuance, additions, changes, re-certifications and deletions to individual access must be approved by the individual's supervisor, appropriate data stewards and/or other parties identified in institutional policy for defined

systems and must have a valid business justification. For example, access to an administrative system may require approval by a user's supervisor and/or a data steward or their delegate with authority to grant access to a system or data environment.

2.2.2 Third Party Access

All third-party access to multi-user systems must be approved by representatives approved by data stewards or their delegates.

Third parties may have administrative/privileged access to systems only with an appropriate business justification and authorization for each affected system.

All third-party accounts on systems that host SI will be deprovisioned without unreasonable delay when the business need for the account no longer exists.

All third parties with access to SI must adhere to all regulations, policies and contractual terms associated with that information (e.g., payment card industry contractual terms, FERPA requirements for student records, HIPAA for protected health information (PHI), and the NC Identity Theft Protection Act for SSNs). Non-disclosure, confidentiality agreements and documentation of compliance must be considered for initial access and on a known schedule thereafter.

2.2.3 Remote Access

All remote access to systems containing SI must be authenticated and the information must be encrypted in transit or have other, effective compensating controls in place.. Access to all information systems must be assessed for appropriateness of security controls to the type and sensitivity of the information involved. Any required actions based on that assessment must be controlled by governance approved by institutional leadership..

2.2.4 Physical Access

Multi-user systems that work with SI and the infrastructure required to support them must be installed in an access-controlled area that includes protection of such devices from physical access by unauthorized individuals.

Procedures or processes must be implemented to audit on a designated frequency users granted access to each area with SI protections in place and to remove access without unreasonable delay based on changes in roles or responsibilities.

2.2.5 Log-in Banner

To the extent technically feasible a log-in banner must be implemented on systems that contain sensitive information such that it displays prior to digital access to sensitive information to declare limits and conditions of access.

2.3 Access Audit and Review

Access review is required for systems that host SI. UNC System units responsible for access-controlled systems must create and follow documented procedures or processes to regularly review individual and system account

access, including review of physical (badge) access. Access must be remediated promptly (as defined by institutional risk-based documentation and governance).

Individuals responsible for access control for each system must review and approve all requests for access modifications.

2.4 Access Rights Management

Access to systems and applications hosting UNC System sensitive information (SI), defined below, must be authorized. Privileged access to systems or applications hosting SI must be individually authorized. Requests for privileged access authorization must be made according to established processes, be based on business need for the access and be re-certified on a schedule specified by each institution.. Authorization for access to systems or applications hosting SI must be revoked without unreasonable delay when an individual's employment status, job function, or responsibilities no longer require those access privileges. Revocation of access along with associated timeframes must be defined in established processes. Authorization of access to non-privileged accounts may be based on user role/group rather than individual authorization.

2.5 Exceptions

Exceptions to this Standard may only be made when confirmed in written form by the Chief Information Officer (CIO) of the UNC System or their delegate(s), authorized in written form. The written form may be submitted electronically.

Access roles only permitting users access to their own information are excluded from the requirement for access review.

Individuals may authorize their own access to development or test systems if they are authorized in a comparable production system to have access to the same data contained in the development or test system for which they are responsible. The development or test systems are not exempt from necessary controls to protect their data from unauthorized access.

3. COMPLIANCE

Each UNC System institution is responsible for assuring compliance via their policies and procedures.

Violation of this Standard may also carry the risk of civil or criminal penalties or contractual consequences.

Failure to comply with this Standard may put UNC System information assets at risk and may have disciplinary consequences, depending on the relationship with the User(s).

Until the effective date, consider this Standard to be advisory best practice. After that date, the Standard will be in full force and effect. Alternatively, institutions may create and retain a compliance plan indicating milestones and compliance dates and any additional resources needed to meet those dates.

4. ROLES AND RESPONSIBILITIES

Business data governance roles defined at each UNC System institution participate in the development and implementation of processes described in this Standard.

Managers of users with access to covered systems participate in this Standard via the authorization, review, and decommissioning of their subordinates' access.

Data stewards and IT service providers support the implementation of access controls, document processes, and participate in requirements defined in this Standard.

5. DEFINITIONS

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources, to gain knowledge of the information the system contains, or to control system components and functions.

Access Controls: Technical tools that limit who is authorized to have an account, what they are authorized to do with their account, and how they are to proceed with accessing the systems which they have permission to use. Access controls are designed to protect both individuals and SI.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges. Privileges are no longer "authorized" when a user leaves a role upon which the authorization was based (for example, leaving a job or changing to a new position with different responsibilities).

Constituent institution: Any member institution of the UNC System, including organizations that report to any UNC System member institution(s).

Data steward: A generic reference here (depending on organization) to an institutional official with responsibility for the protection of and authorization for release of certain types of information (usually sensitive information) defined by relevant information classification policies, procedures or standards.

Measures (as used in BoG 1400.3): actions taken to protect.

Multi-User System: A server or other system providing access or services for more than one concurrent user. Typically, a system that multiple people rely upon to be reliably available for use.

Policy: Policy, Standard, Procedure or other documents specified in institutional policy and governance documentation. Institutional policy is policy relevant to an individual institution that meets or exceeds requirements of BoG 1400.1-3.

Privileged: System or Application Administrators as well as users with elevated data-access privileges (beyond access to their own data) are considered "privileged" users. User accounts with higher privileges than a standard user of an application or operating system or those with access to SI other than their own are considered "privileged" accounts. This includes administrators of servers or multi-user applications, privileged access to applications, or "sudo" access. A user who can set privilege levels for other users is an administrator and therefore "privileged." **NOTE:** for purposes of this Standard, common use of "local-admin" privileges on individual devices are not included.

Role: A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.

Sensitive Information (SI): Information regulated by law, protected by contractual terms or defined in classification and other policies relevant to a UNC System institution.

Standard user: Any UNC System employee, vendor, constituent, student or other individual, including visitors, with access to information technology systems or services that are granted access.

Systems: The physical or logical assets of the IT organization that includes such peripherals as hardware, software, networks, designs, and architectures.

Technique (as used in BoG 1400.3): A way of doing something using special knowledge or skill.

Third-party: Any person or organization that has a contractual agreement for professional services with any constituent institution of the UNC System.

User Manager: A User Manager is any administrator, faculty member, or staff member who supervises Users or who handles business unit administrative responsibilities.

6. RELATED REQUIREMENTS

6.1 University Policies, Standards, and Procedures

- Institutional Information Classification policy that specifies a definition for SI.

7. CONTACT INFORMATION

7.1 Primary Contact

- Chief Information Officer, UNC System
- Email: help@northcarolina.edu

8. References

Internet 2 Trust and Identity in Education and Research (TIER)

National Institute of Standards and Technologies (NIST) SP 800-63 suite of documents